認定NPO法人
日本システム監査人協会報
2016年5月号
No 182
— No.182（2016年5月号）<4月25日発行> ——————————

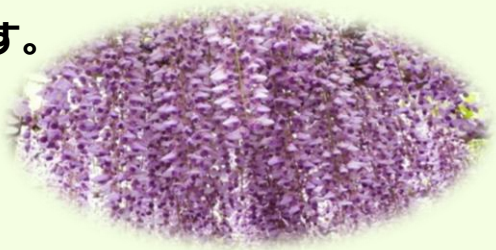
◆ お見舞い ◇◆

熊本県を中心に相次いでおります地震で亡くなられた方々、ご家族や知人が被災された方々、並びに関係者の皆様に対しまして、心よりお見舞い申し上げます。

今月号のテーマは「システム監査の多様性」です。

FinTech、IoT、サイバーセキュリティ・・・・

IT技術の進展等に伴い、リスクが多様化している今日、システム監査はどう対応していけばよいのでしょうか？



写真提供：仲　会長

巻頭言

『 FinTech とシステム監査』

会員番号 608 三谷 慶一郎（副会長）

FinTech（フィンテック）をご存じでしょうか？

FinTech とは Finance と Technology を組み合わせた造語で、IT を活用した革新的な金融サービスの総称のことをいいます。日本でも数年前くらいから多くの FinTech ベンチャーが立ち上がり始めています。複数の銀行口座を管理するサービスや、資産運用における助言を AI 活用によって行うロボ・アドバイザー等、既存の金融機関にはない FinTech サービスが提供され始めています。

興味深いのは金融庁自身が、金融機関に対して FinTech を有効に活用していくことを推奨し始めていることです。「金融行政方針」や、金融審議会のワーキンググループでも、銀行が新しいサービス革新を行っていくために FinTech 企業との連携を進めるべき、というメッセージが提示されています。

既に、金融機関と FinTech 企業とのアライアンスは多く生まれ始めており、API を介して金融機関のサービスと FinTech サービスとをダイレクトに連携させていくことも検討され始めています。

金融業界において新しいイノベーションを起こすことは重要なことで、歓迎される動きだとは考えますが、システム監査人の視点から見ると新しいリスクがそこにはあるように思えます。

金融機関の基幹システムは、ご存じの通り大規模・複雑なもので、品質の確保を最重要視した開発・保守を行っています。一方、FinTech は、新しいサービスを IT で創りだすことが目的で、エンドユーザの反応を見ながら、アジャイル的に更新を繰り返していくことが多く、何よりも開発スピードを重視するものです。

このある意味矛盾する二つの領域にある IT を統合・管理し、全体としての安全性・信頼性を確保するのは容易なことではないでしょう。このあたりにもシステム監査人が取り組むべき新しいテーマが潜んでいるのではないでしょうか。

☞ 関連記事： 投稿 P.5

各行から Ctrl キー+クリックで
該当記事にジャンプできます。

<目次>

2016.4

めだか　【　システム監査の多様性　】

情報化社会という言葉は、今や、IT（Information Technology）社会という言葉に変化している。情報システムは多様化し、ビジネスでの利用から広くコンシューマーが利用する IoT（Internet of Things）、すなわちモノのインターネットと称されるシステムになってきている。「多様性」とは、様々な変化の結果であるが、考えてみると、もっと大きな変化の時代があったことが思い出される。3 月に札幌を旅行する機会があり、北海道大学のキャンパスを訪問した。いうまでもなく、札幌農学校を前身とする大学である。「武士道（Bushido-the soul of Japan）」を 1900 年に著した新渡戸稲造博士が、札幌農学校で学んでいたことはよく知られている。当時の日本は、西洋文明の荒波にもまれる船のような存在であったと思う。

『「武士道」を原文で読む』によると、博士が本書を執筆するきっかけは、「宗教がないのにどうして道徳教育ができるのか（How do you impart moral education?）」と、ベルギー人の法学者ラブレー氏に問い掛けられたことであり、博士は、「私に物事の判断基準を吹き込んだのは武士道であることに気づいた。（I find that it was Bushido that breathed them into my nostrils.）」と書いている。武士道とは、「義、あるいは正義（Rectitude）」「勇気、勇敢と忍耐の精神（Courage）」「仁、惻隠の情（Benevolence）」「礼（Respect）」「真実そして誠実（Honesty）」「名誉（Honor）」「忠義（Loyalty）」の七つの徳に至る武士の道であるとしている。また、「意識はされないが抵抗しがたい力として存在する武士道は、日本と日本人を今も動かし続けている。（An unconscious and irresistible power, Bushido has been moving the nation and individuals.）」とも書いている。

「不易流行」という言葉がある。“いつまでも変化しない本質的なものを忘れない中にも、新しく変化を重ねているものをも取り入れていくこと。また、新味を求めて変化を重ねていく流行性こそが不易の本質であること。蕉風俳諧（しょうふうはいかい）の理念の一つ。解釈には諸説ある。「不易」はいつまでも変わらないこと。「流行」は時代々々に応じて変化すること。”とある。

システムは多様化していくが、核となるシステム監査の考えかた、例えば、リスクとコントロールのアプローチは、変わらないと思う。

（空心菜）

出典：『「武士道」を原文で読む』新渡戸稲造 原著 別冊宝島編集部 編　宝島社新書205

出典：『新明解四字熟語辞典』　三省堂

☞ 関連記事：めだかP.4　投稿P.5

（このコラム文書は、投稿者の個人的な意見表明であり、ＳＡＡＪの見解ではありません。）

<目次>

2016.4

めだか　【　テクノロジーのトップ 10 リスク（システム監査の多様性）】

FinTech、IoT、ビッグデータ、サイバーセキュリティ等々、IT 技術の進展・利用拡大に伴い、組織が抱えるリスクも多様化してきている。こうした様々なリスクにシステム監査は、どのように対応していけばよいのだろうか。そうしたことをいろいろと考えていると、出口の見えない迷路に入っていくような気がしていた。

だが、最近読んだ『月刊監査研究』（日本内部監査協会）に掲載されたレポート(注) が、多様化したリスクに対するシステム監査人としての対応について考えるヒントになったので、ここでご紹介する。

（注）フィリップ・E.フローラ、サジャイ・ライ著、堺咲子訳「テクノロジーのトップ 10 リスクの舵取り―内部監査の役割―」（『月刊監査研究』2016 年 1 月号）：リンク先

このレポートは、2015 年 CBOK 内部監査の実務家国際調査を基に、「テクノロジーのトップ 10 リスク」を決定するとともに、「これらのリスクに関して内部監査人が尋ねるべき重要な質問」「テクノロジーリスクに対処するための重要な業務」について述べている。

世界の内部監査部門長や情報技術専門家へのインタビューの結果、テクノロジーのトップ 10 リスクとして、以下のリスクがあげられている。

①サイバーセキュリティ：近時最も議論されているテクノロジー
②情報セキュリティ：組織にとっての重要な情報の機密性、完全性、可用性の保護
③IT システム開発プロジェクト：IT 予算の大部分はシステム開発プロジェクトに費やされる
④IT ガバナンス：多くの経営者は IT に費やした金額に疑問を抱いている
⑤アウトソースした IT 業務：アウトソースした IT 業務は状況が見えにくくなる
⑥ソーシャルメディアの利用：ソーシャルメディアの方針と手続の制定が必要
⑦モバイルコンピューティング：モバイル機器の普及は労働力に大変革をもたらした
⑧内部監査人の IT スキル：有能な IT 監査人の数の確保は内部監査にとって継続的な課題である
⑨新たなテクノロジー：テクノロジーの変化と発展の速度は驚異的で組織に新たなリスクをもたらす
⑩取締役会と監査役会のテクノロジー認識：取締役会と監査役会に IT 専門家はわずかしかいない

上記のリスクに対する内部監査人の役割や、実際に監査するにあたっての質問事項も記載されており、参考になった。しかし、ここでは紙面の関係でそれらの説明は割愛する。詳しく知りたい方は、前記レポートをご確認いただきたい。

システム監査人として、新しい IT 技術に伴うリスク状況を個別に洗い出すことも必要ではあろうが、そればかりにとらわれず、IT 動向を踏まえながらリスクの全体状況を俯瞰するということも、忘れてはなるまい。

（やじろべえ）

☞ 関連記事：めだかP.3　投稿P.5

（このコラム文書は、投稿者の個人的な意見表明であり、ＳＡＡＪの見解ではありません。）

<目次>

2016.4

投稿　【　システム監査の多様性　】

会員番号　0655 荒牧 裕一（近畿支部）

1．監査形態の多様性と保証業務の概念的枠組み

ICTを利用した情報システムが高度化し適用範囲が広がるに従って、情報システム関連の評価に対する要求も多様化し、システム監査においても従来と違う視点が求められ多様化が進みつつある。

私は、システム監査学会の「システム監査の多様性」研究プロジェクトの主査を務め、ビッグデータ、SNS、知的財産保護、マイナンバー等の多様化する情報システムや監査ニーズについてシステム監査の視点からの研究を行っている。その中で感じたのは、監査の対象の多様化に合わせて監査形態の多様化も必要となるということである。この監査形態については、会計監査の世界では2004年11月29日に「財務情報等に係る保証業務の概念的枠組みに関する意見書」が出されたのをきっかけに、保証業務（システム監査における保証型監査に該当すると考えられる）の形態が分類・体系化された。システム監査の世界ではこのような概念的枠組み（フレームワーク）の公表はされていないが、上記意見書の分類が参考になると思われるので、その内容をシステム監査業務を踏まえながら紹介したい。

2．間接監査（アサーション・ベース）と直接監査（ダイレクト・レポーティング）

「保証型監査では何をどの程度保証べきか」という議論は昔から行われているが、その「何を」に関する一つの解がこの分類である。

財務諸表監査においては経営側の作成した財務諸表を、内部統制監査においては同じく経営側の作成した内部統制報告書を対象とし、そこに表明された情報（アサーション）の信頼性についての意見を表明している。このように、経営側の作成した報告書等の内容を監査して意見表明するのが間接監査（アサーション・ベースの保証業務）であり、会計監査では一般的である。一方、経営側の作成した報告書等を介さずに、監査人が直接に監査テーマについて監査して意見表明をするのが直接監査（ダイレクト・レポーティングの保証業務）である。

システム監査においても、非監査企業の成熟度が高い場合は、内部のシステム監査人がまずシステム監査報告書を作成し、それを対象に外部のシステム監査人が間接監査を行うという形態が理想的であろう。しかし、成熟度が低くてシステム監査報告書を作成するスキルがない場合は、直接監査によらざるを得ない。しかし、直接監査は膨大な時間と手間がかかり、また外部監査人が収集できる監査証拠にも一定の限界があるため、監査の範囲を特定のシステムや事業所に限定したり、後述のように保証の程度の弱い限定的保証を採用するなどの対応が必要になると考えられる。

3．合理的保証（積極形式）と限定的保証（消極形式）

「保証型監査では何をどの程度保証べきか」の「どの程度」に関する一つの解がこの分類である。

合理的保証は、通常の財務諸表監査等で採用されているもので、監査報告書において「財務諸表は全ての重要な点において適正に表示しているものと認める」という形の積極的な文章で記述する。この場合も、保証の程度はあくまで合理的な程度であり、100%の保証ではないことにも注意が必要である。

一方、限定的保証は、四半期財務諸表レビューで採用されているもので、レビュー報告書において「四

半期財務諸表に適正に表示していないと信じさせる事項が全ての重要な点において認められなかった」という非常に間接的・消極的な形の文章で記述する。これは、速報性がより重視される四半期財務諸表レビューでは、監査の期間や収集できる証拠に一定の限界があるため、調べた範囲では問題が認められなかったという程度の限定的な保証しか行えないことによる。また、合理的保証を行う監査と区別するため、「レビュー」と呼んでいる。

システム監査においては、年間契約等により長期間に渉って継続的に監査を行い、システム監査人が必要とする証拠をほぼ無限定に収集できる環境があれば、合理的保証が十分可能であろう。しかし、数日程度の限られた期間で、関係者へのインタビューや関係文書の閲覧等を中心に証拠を収集する手続きであれば、限定的保証に留まらざるを得ないと考えられる。

4．合意された手続（AUP：Agreeed Upon Procedures）

監査やレビューといった保証業務より簡易な手続で行われるのが、合意された手続である。これは、あらかじめ経営側と業務実施人との間で手続の内容について合意をし、その手続のみを実施して結果を報告するものである。監査やレビューではないので、報告書は意見の表明ではなく結果の報告を行う点に注意が必要である。

例えば、個人情報保護法の改正やマイナンバーの実施への対応等が必要な企業が、事前にチェックリストを作成して、各部署がそのチェックリストの内容を遵守しているかどうかを外部の業務実施人が確認していくといったものが、この合意された手続に該当するであろう。

これは、保証業務には該当しないが、特定の目的のために簡易迅速な確認を行う必要がある場合に活用できると考えられる。また、例えば３日間程度の非常に限られた期間しか与えられておらず、上述のレビューによる限定的保証ですら難しい場合は、当初から合意された手続を選択した方が良い場合もあると考えられる。

5．まとめ

システム監査においても監査目的や監査対象に応じて、多様な監査形態を採用していく必要性を感じ、会計監査における保証業務の概念的枠組みを紹介し、システム監査への適用を考えてみた。

しかしこれはあくまでも参考であり、会計監査での分類や用語をそのままシステム監査に適用すべきだというものではない。また、会計監査においても今後この枠組みは変化していく可能性がある。

システム監査技術者試験では、監査論の分野の出題がほとんどないこともあり、システム監査人のほとんどは監査論について体系的に学習したことはなく、また学習したくてもシステム監査に特化した監査論の資料や研修はほとんどないのが実情であろう。したがって、先行している会計監査の体系もある程度は参考になると考えられる。

今後、システム監査の多様性が進むにしたがって、監査形態も多様化し、システム監査独自の概念的枠組みが作られる日が来ることを期待している。

☞ 関連記事
巻頭言 P.1 | めだか P.3 | めだか P.4 | 本部報告 P.8 | 本部報告 P.13 | 支部報告 P.18 | 注目情報 P.23

<目次>

2016.4

投稿　【　システム監査の活性化　】

会員番号　0557 仲厚吉（会長）

1．システム監査を核にして

当協会では、第15期通常総会で事業計画が承認され、2016年度の事業活動を開始しています。また、2016年度より、次に挙げる「SAAJのビジョン（3年後に目指す姿）」を掲げました。事務局をはじめ、各委員会、部会研究会が、それぞれ3か年で目指す目標を定めシステム監査の活性化を進めていきます。

●社会の多様な要請に対応し、信頼性・安全性が高くかつ有効なIT活用を実現することを目標として、ITサービスの提供者と利用者双方における適切な統制を維持・向上させる活動を、既存のシステム監査を核にした“ITアセスメント”としてとらえる。
そのうえで、SAAJの活動を“ITアセスメント”の定着に焦点を当てて取り組む。
●これにより、会員を含むシステム監査人のビジネス機会の増大を図り、SAAJの知名度向上、会員の拡大に繋げる。

2．社会の多様な要請に応える

朝日新聞朝刊（2016年3月30日）に、「ベネッセ顧客情報流出 元SEに実刑判決 東京地裁支部」という見出しで次のような記事がありました。

通信教育大手ベネッセホールディングスの顧客情報流出事件で、不正競争防止法違反の罪に問われた元システムエンジニアの被告（41）に対し、東京地裁立川支部は29日、懲役6カ月、罰金300万円（求刑懲役5年、罰金300万円）の判決を言い渡した。裁判長は「専門知識を悪用して極めて大量の顧客情報を得ており、悪質な犯行。情報を売って得た利益を競艇に使っており、動機は身勝手かつ短絡的だ」などと述べた。判決によると、被告は勤務先だったベネッセ子会社の多摩事業所（東京都多摩市）内で、顧客データベースに接続。名前や生年月日、住所などの情報約3千万件を自分のスマートフォンに転送し、うち約1千万件を名簿業者に渡した。

「情報処理システム監査」と言われた時代、システム監査人は、メインフレームと呼ばれる汎用機を利用した情報処理システムの監査に当たっていました。2016年1月から、マイナンバー法の施行が始まりましたが、ビッグデータの利活用などのため、個人情報の保護と利活用、プライバシー・バイ・デザイン、情報セキュリティ、事業継続が課題になっています。社会の多様な要請に応えていくことが、システム監査の活性化や、SAAJの活動を“ITアセスメント”の定着に焦点を当てて取り組んでいくことに繋がります。

以上

<目次>

2016.4

第211回月例研究会講演録　【　クラウドサービスのセキュリティ規格ISO/IEC27017　】

会員番号　2564　櫻井 俊裕

講師　：　特定非営利活動法人　日本情報セキュリティ監査協会
　　公認情報セキュリティ主席監査人　事務局長　永宮 直史 氏

日時、場所　：　2016年3月2日（水）18：00 – 20:00、機械振興会館　地下2階ホール（神谷町）

テーマ　：　「クラウドサービスのセキュリティ規格ISO/IEC27017」

要旨：

2015年12月に発行のISO/IEC27017は、経済産業省の「クラウドサービス利用のための情報セキュリティマネジメントガイドライン」を下敷きに、日本の提案により規格化された。ISO/IEC27002をベースに、クラウドサービス固有の管理策や実施の手引きを記載したISO/IEC27017、その狙いとその特徴を解説する。

講演録：

1．クラウドサービス固有のセキュリティ規格の必要性

クラウドサービスは、従来のコンピュータシステムとは異なるパラダイムであり、その違いから固有のセキュリティ規格の必要性が叫ばれた。それに対し、日本がいち早く提案を行い、主導することでISO/IEC27017は作成された。

クラウドサービスのセキュリティは利用者と事業者の共同責任である。事業者が一定の決まりの下でセキュリティ環境を用意し、利用者はその環境を良く理解した上で必要なセキュリティ対策を施す。ISO27017は、事業者と利用者のコミュニケーションを円滑にし、そのコミュニケーションに基づきセキュリティを確保するという考え方で作られた。

27017で使用されている用語は、以下のISO/IEC17788の定義を引用している。

【ISO/IEC 17788:2014】

3.2.5 cloud computing: Paradigm for enabling network access to a scalable and elastic pool of shareable physical or virtual resources with self-service provisioning and administration on-demand.

Note – Examples of resources include servers, operating systems, networks, applications, and storage equipment.

クラウドコンピューティングとは、オンデマンドで自らが供給し管理し得る、共有された物理または仮想リソースの柔軟な拡張性に富むプールへのネットワークアクセスを可能にするパラダイムである。リソースとは、サーバ、オペレーティングシステム、ネットワーク、アプリケーション、および記憶装置を

含むもの。として規定されている。ここでは、コンピュータ技術の定義では無く、どういった使い方をするかが述べられている。

【ISO/IEC 17788:2014】

3.2.8 cloud service: One or more capabilities offered via cloud computing (3.2.5) invoked using a defined interface.

クラウドサービスとは、規定されたインターフェースを利用することで動作するクラウド・コンピューティング（3.2.5に記載）により提供される、一つまたは複数の機能と規定されている。

ここでいうcapabilitiesとは機能と訳す。ISOではクラウドサービスの分類を、SaaS/PaaS/IaaSの他、Application capability / Platform capability / Infrastructure capability　という機能別の分類を併用しており、この機能を意味している。

クラウドサービスの利用者側の定義として、Cloud Service Customer はクラウドを利用する組織を指し、組織と個人との混同を避けるため、日本語訳では“クラウドサービス利用者”では無く、“クラウドサービスカスタマ”と表現する。また、Cloud Service User とはクラウドサービスの端末を操作する人を指している。クラウドサービスの提供者側の定義として、Cloud Service Provider はクラウドを提供する組織を指し、日本語訳では“クラウドサービスプロバイダ”と表現する。Peer Cloud Service Providerとはサプライチェーンの上流サービスを提供するプロバイダを指す。

オンプレミスからクラウドサービスまでのサービス形態は、その違いにより以下の様に定義されている。

・オンプレミス・・・利用者が管理する場所で、利用者自身が所有する情報機器を利用する形態。
・ハウジング・・・提供者が管理する場所で、利用者自身が所有する情報機器を利用する形態。
・ホスティング・・・提供者が管理する場所で、提供者が所有する情報機器を、利用者が専用で利用する形態。
・クラウド・・・提供者が管理する場所で、提供者が所有する情報機器を、利用者が他の利用者と共同で利用する形態。特に非常に大きなリソースを持ち、利用者の必要に応じた容易な拡張を可能としている。

例）クラウドサービスで最もヘビーユーザであるゲーム業界では、キャンペーン期間に膨大なトランザクションが集中し、一時間に数千台のサーバ追加が必要となり、数日後には不要となるようなケースがある。

商用システムでは、オンプレミスからクラウドサービスへ移行することで、容易な拡張性とシステム管理面での膨大な省力化が可能となる。その際、サービス提供者は特定の利用者に対する要求は受けない為、利用者側でセキュリティ機能や変更管理内容等の正確な情報提供を受け、提供者側が実施しない作業を行

う必要がある。

従って、クラウドサービスにおいては、利用者と提供者間の明確な責任分解が定められ、提供者から利用者に向けて、サービスに関する正確な情報とコミットメントがなされる事が重要であり、利用者と提供者双方の情報セキュリティマネジメントを成り立たせるために、提供者から利用者へのサービスマネジメント的な情報提供が必要となる。

また、仮想マシンのライブマイグレーション機能は資源の有効活用とシステムの冗長化に役立つが、システム切り替え時の適切な措置を講じないと、大規模な事故に発展するリスクがある。リスク回避の為、前述の利用者と提供者との関係の定義に加え、この様なクラウド固有の技術的な管理策を定めておく必要がある。

本規格を使いこなすには、利用者がクラウドにおけるレイヤー毎のリスク対策について、理解している必要がある。

２． ISO/IEC27017の概要

(1)ISO/IEC27017作成経緯

ISO/IEC27001:2005 ISMS Requirements, ISO/IEC27001:2005 Code of Practice を基に、経産省にて“情報セキュリティ管理基準（2003年策定、2008年改訂）”が策定された。2011年4月に、クラウド利用者目線に立った“クラウドサービス利用者のための情報セキュリティマネジメントガイドライン”が、同じく経産省にて策定された。

日本は本ガイドラインを2010年にISOベルリン会合にてプレゼンによる提案を実施している。翌々年のISOナイロビ会合では、元来クラウド利用者視点の内容に対しクラウド事業者側の視点が盛り込まれた。

その後、2013年10月にISO27001自体の大幅改変の影響で作業が遅れ、2015年12月にISO27017:2015 Cloud Computing として完成に至った。

(2)ISO/IEC27017と関連規格

ISO27000ファミリーの中で、27017の関連企画としては以下のものがある。

- ISO27018・・・クラウド事業者がPII（個人識別情報）を預かる時の定義である。プライバシーデータを扱う際のコントローラ（クラウド利用者）とプロセッサ（クラウド事業者）間の橋渡し規格。
- ISO27036-4・・・供給者関係の技術的な取り決めの規格。システムライフサイクルに従い、利用者と事業者間の契約事項について定義しており、現在作成中。
- ISO19086-4・・・SLAの基準を検討中。
- SP CS use cases・・・クラウドサービスのセキュリティ管理に手を加える部分が無いかを、日本の提案で検討中。

以上の枠組みの中で、一番の中心が27017となっており、これはITUTとの共同文書として発行され、クラウドについては米国CSA（Cloud Security Alliance）と共に策定されている。

(3)全体構成

全体構成はISO/IEC27002（以下、27002）と同じ構成とした。適用範囲から引用規格は全く同じとし、4項にクラウド固有の概念を記載した。管理策は27002と変わらないが、27002に欠けた部分を“クラウドサービス提供者／利用者の為の実施の手引き関連情報”に補記した。クラウド固有の管理策については“付属書A（規定）クラウドサービス拡張管理策集”を追加した。リスクについては本編に入れたかったが、リスクに対する考え方が世界で異なるため、“付属書B（参考）クラウドコンピューティングの情報セキュリティリスクに関する参考文献”として記載した。

管理策全体の約3分の1弱にクラウドに関連した内容が記載される結果となった。

(4)ISO/IEC27017の追加管理策

以下の7つの管理策が追加された。

・CLD.6.3.1　役割と責任の分担・・・英語ではshared、責任は共有するが役割を分担する。

・CLD.8.1.5　CSCの資産の除去・・・仮想のメモリ上の資産は返却困難であり、確実に除去（消す）を行う。

・CLD.9.5.1　仮想コンピューティング環境における分離・・・1顧客の利用領域が確実の他と分離する。

・CLD.9.5.2　仮想マシンの要塞化・・・未使用のサービスやポートへの攻撃防止を考える。

・CLD.12.1.5　実務管理者の運用のセキュリティ・・・オペレーションミスの防止。

・CLD.12.4.5　クラウドサービスの監視。

・CLD.13.1.4　仮想及び物理ネットワークのセキュリティ管理の整合。

(5)記載のしかた

27017ではISO2736の記載方法に合わせて、“クラウドサービス利用者”と“クラウドサービス提供者”双方の実施手引きを対比して記載している。提供者からのサービス機能に関する情報を、利用者が入手した上でリスク分析を行い、自らが望むセユリティレベル達成への必要な作業を実施する、という表現形式をとっている。

27027では、27002の一般的な情報セキュリティ対策に加えて、クラウド利用者には「事業者提供情報・機能の確認」及び「クラウド利用上の注意事項」を、クラウド提供者には「技術的対策」、「契約上の課題対策」等、及び、利用者とのコミュニケーションとして「利用者の情報セキュリティ対策支援（情報・機能の提供）」を、クラウド固有の対策として新たに定義した。

クラウドのための実施手引きとして、まずISO/IEC27001に基づくマネジメントシステムを確立し、リスクマネジメントを実施する。次に27002に定義される一般的な管理策及び27017のクラウド固有の管理策を実装する流れとなる。　提供者における、クラウドサービスのリスクアセスメントでは、組織的視点に加えて、供給者自身や顧客に目を向けた事業的視点での分析が必要となる。

また、クラウドサービスに限った事では無いために27017には記載されていないものの、ベンダーロックインのリスクについても考慮が必要である。

３．ISO/IEC27017の内容（例）

講師希望により、講演録省略。

４．今後のISO/IEC27017

(1) JIS化・・・早ければ今年一杯、遅ければ来年の見込み。

(2)認証制度・・・ISMSの適合評価制度に乗せるべくJIPDECと調整中。プライベート認証においてISO27018事例ではコントロールの数が120に対し監査項目数が1,000項目弱であり、半年以上かけて非常に詳細な審査を実施している。今のISMSがそれに耐えられるかは問題である。今後国際的な監査の整合性をとる為には、監査の充実が必要である。国際的にクラウドサービスを展開するのであれば、グローバルスタンダードな審査を通過しているという形にしたい。

(3)監査技法（ISO/IEC TR 27008）・・・日本のテクニカルな部分の監査レベルをグローバルに説明可能とするため、監査の方法を27008に記載予定。

(4)監査の普及・・・上記により、監査全体の普及を目指す。

(5)改善・・・以下4点について改善を考えており、数年がかりでも良いものにしていきたい。

①要求事項（ISO/IEC27009）・・・27017はあくまでも27002の拡張でありガイドラインに過ぎない。通常の認証の審査からいうと、コントロールレベルで追加するところのみ見てしまうという過ちを犯す懸念がある。きちんとした要求事項の総体としてクラウドのリスク分析を行い管理する仕組みができれば、ISO/IEC27009をベースとした要求事項としてのスタンダードに合わせることができる。その様な長期的な考慮に基づく制度設計が必要であり、それによって日本は世界とのレベルを合わせた認証が可能となる。

②クラウド仲介業者への対応（SIer、仲介業者など）

③欠落している事項への対応・・・ユーザアプリケーション検証環境が少なく利用が阻害される問題、監査の問題等。

④構造的な改善・・・その場の議論で論理的にすっきりしていない部分がある。

感想：

クラウド社会を支える上で必要となるコントロールについて、非常に理解しやすく解説頂き、価値ある内容でした。特に本規格が、日本の主導で進められたことは、日本クラウドビジネスのグローバル展開において有意義であり、これからの活動を見守ると共に、必要な協力を行いたいと考えました。

以上

☞ 関連記事： 投稿 P.5

<目次>

2016.4

第28回ＣＳＡフォーラム開催【システム監査を巡る今日的課題】

会員番号　2581 斉藤 茂雄（CSA 利用推進 G）

今回は、日本大学商学部教授で商学博士の堀江正之先生を講師に迎えました。堀江先生は、システム監査の理論研究や内部統制、ITガバナンス、情報セキュリティガバナンスなどに造詣が深く、研究、著述、学会、ご講演等で幅広くご活動なされております。

今回はこれまでと会場を変えて実施しましたが、「システム監査を巡る今日的課題」というテーマと、システム監査の外部環境が大きく変貌しているということから、30名の皆様にお集まりいただきました。

私など、企業の内部監査人として、見よう見まねで監査を実施して来た者には、今回のお話は「監査のあり方」に立ち帰る、非常に有益な内容でした。また先生は「システム監査基準」の作成にも携わったということで、監査基準の成り立ちなど、興味深いお話もうかがえ、大変貴重な２時間でした。

開催の概要は以下です。終了後講師を囲んで短時間ですが懇親会を実施しました。

タイトル：「システム監査を巡る今日的課題」
概要；（当日使用スライドのコンテンツより一部抜粋）：

実務上の課題

標的型メール攻撃の増加を受けて・・・・/　サイバー攻撃に対する監査の考え方/
情報漏洩を例にしたシステム監査人の目線ー組織のための監査と顧客のための監査ー/
サイバーセキュリティに関する情報開示/　サイバー攻撃に対する監査の考え方/
CSIRT とシステム監査/　CSIRT のサービスリストの例/　CSIRT と内部監査部門の位置づけ/
スマートデバイス監査の２つの段階と２つの視点/　SNS 監査の２つの段階と２つの視点/
ビッグデータ監査のポイント/　外部委託の監査の考え方/　委託元における委託管理監査のポイント
マイナンバー対応支援サービス/　委託先の監督/　委託先の適切な選定/
安全管理措置を遵守させるための契約内容/　委託先における特定個人情報の取扱状況の把握/
再委託・再々委託先に対する監督/　マイナンバー制度に係る監査の今後の展開/

理論上の課題

システム監査職能展開の方向性/　深みのあるシステム監査と監査態勢の整備/
システム監査の品質はどう考えるべきか/　監査の最低品質と魅力品質の関係/　監査品質決定要因/
直列型と並列型の監査品質保証体制/　チェックを重ねることで監査品質は向上するか？/
監査品質を高めるための評価方式/　報告様式からみた保証意見と助言意見の違い/
システム監査の２つの職能/　監査でどこまで踏み込むか/　ガバナンスシフトがもたらす意味/

開催日時： 2016 年 3 月 23 日（水）　18 時 30 分～20 時 30 分
開催場所： 中央区日本橋兜町 12-7 兜町第 3 ビル　NATULUCK 茅場町新館 2 階大会議室

☞ 関連記事：投稿 P.5

ＣＳＡフォーラムはＣＳＡ・ＡＳＡの皆様が、「システム監査に関する実務や事例研究、理論研究等」を通して、システム監査業務に役に立つ研究を行う場です。ＣＳＡ・ＡＳＡ同士のフェイスｔｏフェイスの交流を図ることにより、相互啓発や情報交換を行い、ＣＳＡ・ＡＳＡのスキルを高め、よってＣＳＡ・ＡＳＡのステータス向上を図ります。ご参加のお問い合わせはＣＳＡフォーラム事務局：csa@saaj.jp まで（@は小文字変換要）

ＣＳＡ利用推進Ｇのキャッチフレーズ
＊＊ＣＳＡ・ＡＳＡを取得してさらに良かったと思ってもらえる資格にしましょう！！

＜目次＞

2016.4

事例研究会報告　【　第27回システム監査実務セミナー　】

会員番号　1816 野田 正勝（システム監査事例研究会）

３月５日・６日および１９日・２０日の延べ４日間で、第27回システム監査実務セミナーを晴海グランドホテルで開催しました。

今回は５名の受講者を迎え、鈴木（実）講師、野田の２名体制で臨みました。このセミナーは、「システム監査普及サービス」で実施した実際のケースをもとに、事例研究会が教材化したものです。被監査企業の登場人物を講師が務めるロールプレイング形式の演習を中心に構成されており、受講者は監査チームを組んで、まさに監査の疑似体験ができる大変ユニークなセミナーです。

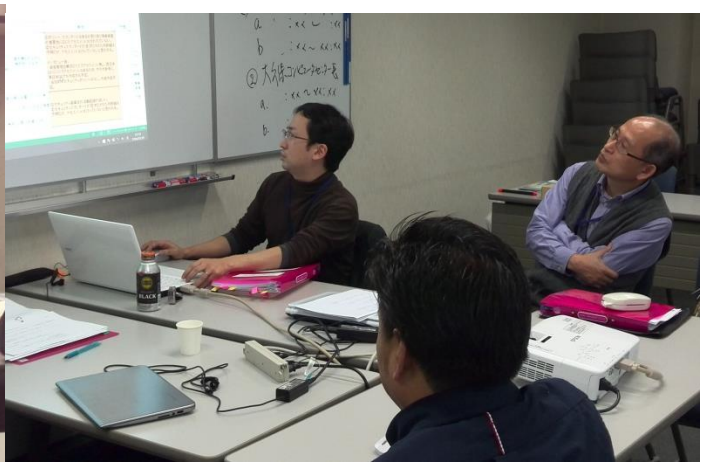
教材は「金融系データセンタにおけるシステム運用に関する監査」のケースを使用しました。

今回の参加者は、システム監査に関する資格や試験に合格済みの方や、日常業務で監査に係る業務を行っている方々がほとんどで、監査の手順については一通り理解されていたためか、演習はスムーズに進行しました。とは言っても、時間が少ないなか、依頼人の要求に答えるべく、監査テーマ・監査項目の設定や、予備調査・本調査を通した問題点の把握に相当苦労している様子は、いつもの通り変わりませんでした。そこが、実際のケースを使用しているこのセミナーならではの醍醐味であり、そのことがまた、受講者の満足度にもつながっているのだと思います。

日中、ハードな演習をこなした後、夜には日付が変わるぐらいまで懇親を深められるのも、このセミナーの良いところです。

次回は９月ごろの開催を計画しています。

（セミナー風景）



<目次>

2016.4

「新個人情報保護法」がＰＭＳに及ぼす影響　～ＰＭＳハンドブック読者！必読！～　　第1回

会員番号　1760 斎藤由紀子（個人情報保護監査研究会）

１．2015 年９月９日「個人情報の保護に関する法律」改正

「**番号利用法**＝行政手続における特定の個人を識別するための番号の利用等に関する法律」第６章に定められていた、特定個人情報保護委員会が、名称を改めて、「個人情報の保護に関する法律（以下、個人情報保護法と呼ぶ）」第５章に、**個人情報保護委員会**　として定められました。

同時に「消費者庁及び消費者委員会設置法」第４条から、”個人情報の保護に関する基本方針の策定及び推進”の任務が削除され、また、第６条の消費者委員会から、”個人情報の適正な取扱いの確保に関する重要事項”の審議が削除され、**2016年1月1日より、個人情報保護委員会が新個人情報保護法の所管となりました。**

今月号から、「新個人情報保護法」が個人情報保護マネジメントシステム（以下PMSと呼ぶ）に及ぼす影響について解説を連載します。

目次　★注目！　※条項番号は全面施行後のもの	
「個人情報の保護に関する法律」2015年9月9日改正	**会報掲載予定**
第一章　総則（第1条―第3条）	2016年5月号
第二章　国及び地方公共団体の責務等（第4条―第6条）	2016年6月号　予定
第三章　個人情報の保護に関する施策等	
第一節　個人情報の保護に関する基本方針（第7条）	
第二節　国の施策（第8条―第10条）	
第三節　地方公共団体の施策（第11条―第13条）	
第四節　国及び地方公共団体の協力（第14条）	
第四章　個人情報取扱事業者の義務等	2016年7月号　予定
第一節　個人情報取扱事業者の義務（第15条―第35条）	
第二節　匿名加工情報取扱事業者等の義務（第36条―第39条）★	2016年8月号　予定
第三節　監督（第40条－第46条）	
第四節　民間団体による個人情報の保護の推進（第47条―第58条）	
第五章　個人情報保護委員会（第59条―第74条）　★	2016年9月号　予定
第六章　雑則（第75条―第81条）	
第七章　罰則（第82条―第88条）　★	2016年10月号　予定
附則　（2015年9月9日法律第65号）	

【表記について】読みやすさの点から、一部漢数字をアラビア数字、和暦を西暦で記載しています。

【本文について】今回は、改正点に絞って解説します。従来から記述されている場合は省略することになりますが、ご了承ください。改正箇所は「赤字」で記載します。

【施行日について】附則第１条に施行日が定められていますが、第２項、第３項に規定するほかは、”この法律は、**公布の日から起算して２年を超えない範囲内において政令で定める日から施行する。**”　ことになっています。

第２項【交付の日から施行】

第10条（個人情報の適正な取扱いを確保するための措置）

第12条（区域内の事業者等への支援）

附則　第7条（委員長又は委員の任命等に関する経過措置）**第２項**

第３項【2016年１月１日から施行】

第１条（目的）、**第４条**（国の責務）、**第６条**（法制上の措置等）

第７条第1項（基本方針）及び**第3項**（基本方針の閣議決定）

第８条（地方公共団体等への支援）、**第９条**（苦情処理のための措置）

第13条（苦情の処理のあっせん等）、**第22条**（委託先の監督）

第25条（開示）、**第26条**（訂正等）、**第27条**（利用停止等）、**第30条**（手数料）

第32条（報告の徴収）、**第34条**（勧告及び命令）、**第37条**（認定個人情報保護団体の認定）

附則第５条（特定個人情報保護委員会がした処分等に関する経過措置）

※上記のうち、**第25条**以降は、施行時に条項番号が変更となる予定です。

例：第25条→第28条　など

※基本方針は、2016年2月19日に一部変更されました。

http://www.ppc.go.jp/files/pdf/280219_personal_basicpolicy.pdf

それでは、今回は、第一章　総則　について解説します。

第一章　総則

第1条（目的）

この法律は、高度情報通信社会の進展に伴い個人情報の利用が著しく拡大していることに鑑み、個人情報の適正な取扱いに関し、基本理念及び政府による基本方針の作成その他の個人情報の保護に関する施策の基本となる事項を定め、国及び地方公共団体の責務等を明らかにするとともに、個人情報を取り扱う事業者の遵守すべき義務等を定めることにより個人情報の適正かつ効果的な活用が新たな**産業の創出**並びに活力ある経済社会及び豊かな国民生活の実現に資するものであることその他の個人情報の有用性に配慮しつつ、個人の権利利益を保護することを目的とする。

※国際競争に立ち向かうため不可欠な、ビッグデータの活用が、”**産業の創出**”　の言葉に表れています。

第2条（定義）
この法律において「個人情報」とは、生存する個人に関する情報であって、次の各号のいずれかに該当するものをいう。
一　当該情報に含まれる氏名、生年月日その他の記述等（文書、図画若しくは電磁的記録（電磁的方式（電子的方式、磁気的方式その他人の知覚によっては認識することができない方式をいう。次項第二号において同じ。）で作られる記録をいう。第十八条第二項において同じ。）に記載され、若しくは記録され、又は音声、動作その他の方法を用いて表された一切の事項（**（個人識別符号を除く。）**をいう。以下同じ。）により特定の個人を識別することができるもの（他の情報と容易に照合することができ、それにより特定の個人を識別することができることとなるものを含む。）
二　**個人識別符号**が含まれるもの

※第一項は、従来通りの考え方ですが、（個人識別符号を除く）とされ、第二項に、個人識別符号のみが別扱いとなりました。

2　この法律において「**個人識別符号**」とは、次の各号のいずれかに該当する文字、番号、記号その他の符号のうち、政令で定めるものをいう。
一　特定の個人の身体の一部の特徴を電子計算機の用に供するために変換した文字、番号、記号その他の符号であって、当該特定の個人を識別することができるもの
二　個人に提供される役務の利用若しくは個人に販売される商品の購入に関し割り当てられ、又は個人に発行されるカードその他の書類に記載され、若しくは電磁的方式により記録された文字、番号、記号その他の符号であって、その利用者若しくは購入者又は発行を受ける者ごとに異なるものとなるように割り当てられ、又は記載され、若しくは記録されることにより、特定の利用者若しくは購入者又は発行を受ける者を識別することができるもの

※第一項は、顔認識・指紋データ等の生体情報、第二項はカード等のID、免許証番号・パスポート等の符号・番号が想定されており、今後、具体的に政令等で定められる予定です。
個人番号も「個人識別符号」のひとつです。

3　この法律において「**要配慮個人情報**」とは、本人の人種、信条、社会的身分、病歴、犯罪の経歴、犯罪により害を被った事実その他本人に対する不当な差別、偏見その他の不利益が生じないようにその取扱いに特に配慮を要するものとして政令で定める記述等が含まれる個人情報をいう。

※JIS Q15001:2006における「特定の機微な個人情報」と比較すると、宗教、身体・精神障害、勤労者の団結権、保健医療が含まれていませんが、不当な差別等が生じないよう配慮を要するものとして、理由がより明確になりました。

※今後、具体的に政令で定められ、本人同意のない取得は原則禁止されます。（第17条）

4　この法律において「個人情報データベース等」とは、個人情報を含む情報の集合物であって、次に掲げるもの（利用方法からみて個人の権利利益を害するおそれが少ないものとして政令で定めるものを除く。）をいう。

※「個人情報データベース等」のうち、一定の規則で匿名化したものを、第三者提供できるようにするため、カッコ書きが追加されました。

9　この法律において「**匿名加工情報**」とは、次の各号に掲げる個人情報の区分に応じて当該各号に定める措置を講じて特定の個人を識別することができないように個人情報を加工して得られる個人に関する情報であって、当該個人情報を復元することができないようにしたものをいう。
一　第一項第一号に該当する個人情報　当該個人情報に含まれる記述等の一部を削除すること（当該一部の記述等を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。
二　第一項第二号に該当する個人情報　当該個人情報に含まれる個人識別符号の全部を削除すること（当該個人識別符号を復元することのできる規則性を有しない方法により他の記述等に置き換えることを含む。）。

※「匿名加工情報」は、復元することができないよう、個人情報保護委員会規則で定める基準に従うことになります。また、匿名だからといって自由に取り扱ってよいというものではなく、さまざまな制約が設けられています。詳しくは、第４章第2節　匿名加工情報取扱事業者等の義務（第36条―第39条 ）で解説します。

10　この法律において「**匿名加工情報取扱事業者**」とは、匿名加工情報を含む情報の集合物であって、特定の匿名加工情報を電子計算機を用いて検索することができるように体系的に構成したものその他特定の匿名加工情報を容易に検索することができるように体系的に構成したものとして政令で定めるもの（第三十六条第一項において「**匿名加工情報データベース等**」という。）を事業の用に供している者をいう。ただし、第五項各号に掲げる者を除く。

※「匿名加工情報」として認められれば、「匿名加工情報取扱事業者」は本人の同意なく第三者提供が可能となります。しかし、どのような個人情報を匿名化したのかを公表するなど、いくつかの義務が課せられることになります。（詳細：第４章第2節で解説）

※第五項各号に掲げる者とは、国の機関、地方公共団体、独立行政法人等、地方独立行政法人をいいます。

第２条（定義）の改定部分は、2016年4月現在未施行です。今後、政令または個人情報保護委員会規則等で詳細が定められる予定で、ＰＭＳへの影響はもう少し先のこととなりますが、まずは用語に慣れておきましょう。

・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・・

次回は、「第２章　国及び地方公共団体の責務等（第４条―第６条）」から解説します。

バックナンバー目次 ＝　http://1.33.170.249/saajpmsHoritsu/000PIPHoritsu.html

！！「ＰＭＳハンドブック」の読者専用ダウンロードサイトでは、第２条で新たに規定された用語について、「3301個人情報取扱規程」に追加し、2016年5月1日公開予定です。！！

SAAJ「ＰＭＳハンドブック」ご紹介サイト：http://www.saaj.or.jp/shibu/kojin.html

認定NPO法人日本システム監査人協会　個人情報保護監査研究会　■

<目次>

2016.4

北信越支部報告【北信越支部2016年度 支部総会・研究報告】

会員番号　1281 宮本 茂明（北信越支部）

以下のとおり2016年度 北信越支部総会を開催しました。

・日時：2016年3月12日（土） 13:00-17:00　　参加者：11名

・会場：富山県民会館

・議題：１．2016年度北信越支部総会

２．本部総会参加報告

３．研究報告

①「サイバーセキュリティ経営ガイドライン　～　仏造って魂入れる　～　」

梶川　明美 様

②「標的型攻撃について」

森　広志 様

４．西日本支部合同研究会 北信越支部報告検討：システム開発/構築に関わるシステム監査

◇研究報告 1

「サイバーセキュリティ経営ガイドライン　～　仏造って魂入れる　～　」

報告者 (会員番号　947　梶川 明美)

１．はじめに

様々なビジネスの現場において、ＩＴの利活用は企業に不可欠なものとなっているが、企業が保有する顧客の個人情報や重要な技術情報等を狙うサイバー攻撃は増加傾向にあり、その手口は巧妙化している。これらに対し、ＩＴに対する投資やセキュリティに対する投資等をどの程度行うかなど、経営者による判断が必要となっている。

経済産業省では、独立行政法人情報処理推進機構（ＩＰＡ）とともに、大企業及び中小企業（小規模事業者除く）のうち、ＩＴに関するシステムやサービス等を供給する企業及び経営戦略上ＩＴの利活用が不可欠である企業の経営者を対象に、経営者のリーダーシップの下で、サイバーセキュリティ対策を推進するため、「サイバーセキュリティ経営ガイドライン」を策定した。 サイバー攻撃から企業を守る観点で、経営者が認識する必要のある「３原則」、及び経営者が情報セキュリティ対策を実施する上での責任者となる担当幹部に指示すべき「重要１０項目」がまとめられている。

２．サイバーセキュリティ経営の３原則

(1) 経営者は、IT活用を推進する中で、サイバーセキュリティリスクを認識し、リーダーシップによって対策を進めることが必要

(2) 自社は勿論のこと、系列企業やサプライチェーンのビジネスパートナー、ITシステム管理の委託先を

含めたセキュリティ対策が必要

(3) 平時及び緊急時のいずれにおいても、サイバーセキュリティリスクや対策、対応に係る情報の開示など、関係者との適切なコミュニケーションが必要

3．サイバーセキュリティ経営の重要１０項目

(1) リーダーシップの表明と体制の構築

①サイバーセキュリティリスクの認識、組織全体での対応の策定

②サイバーセキュリティリスク管理体制の構築

(2) サイバーセキュリティリスク管理の枠組み決定

③サイバーセキュリティリスクの把握と実現するセキュリティレベルを踏まえた目標と計画の策定

④サイバーセキュリティ対策フレームワーク構築（PDCA）と対策の開示

⑤系列企業や、サプライチェーンのビジネスパートナーを含めたサイバーセキュリティ対策の実施及び状況把握

(3) リスクを踏まえた攻撃を防ぐための事前対策

⑥サイバーセキュリティ対策のための資源（予算、人材等）確保

⑦ITシステム管理の外部委託範囲の特定と当該委託先のサイバーセキュリティ確保

⑧情報共有活動への参加を通じた攻撃情報の入手とその有効活用のための環境整備

(4) サイバー攻撃を受けた場合に備えた準備

⑨緊急時の対応体制（緊急連絡先や初動対応マニュアル、CSIRT）の整備、定期的かつ実践的な演習の実施

⑩被害発覚後の通知先や開示が必要な情報の把握、経営者による説明のための準備

4．考察

本ガイドラインを実施していくには、監査人やＩＴ技術者の知見が必要と思われる。システム監査人の有益性をアピールする努力もしつつ、我々の活躍の場が広がることを期待したい。

(1) 監査について

ＩＴシステム管理の外部委託について、当該委託先への監査を実施とあるが、監査できる体制が必要であり、監査自体を委託するか？企業にとっては監査だけでは魅力が乏しく、改善提案の実施に向けたコンサルも要望されるのではないか。

(2) 情報共有活動への参加

情報共有活動へ参加して経営側に説明し、実装していくまでをやり遂げられる人材を内部で育成していくのはかなり大変だと思う。人材育成は永遠のテーマである。

(3) 情報公開

経営者による情報公開としての説明は、技術等について経営者自身が理解することが必要。また、適切なタイミングや公表内容などには、危機管理を含むセンスが必要である。専門家（ＩＴ技術者、弁

護士など）の助言が望ましい。

【参考文献】

- 「サイバーセキュリティ経営ガイドライン」Ver1.0
  平成27年12月28日　経済産業省，独立行政法人情報処理推進機構
  http://www.meti.go.jp/press/2015/12/20151228002/20151228002.html

◇研究報告　2

「標的型攻撃について」

報告者 (会員番号　848　森　広志)

1．標的型攻撃について

標的型攻撃は、サイバー攻撃の1種ですが、計画・組織的な攻撃であり、現存する個々の攻撃手法やツールを場面毎に活用できるよう体系的な準備がなされていると共に、攻撃対象組織向けのカスタマイズが柔軟に行え、個々の手法改善や追加により、更に脅威度合いを増すことができる手強い攻撃手法と考えます。以下は、標的型攻撃の工程概要(例)を推測したものです。

（1）事前調査・準備：①ターゲット組織の絞り込み、組織の調査分析、②セキュリティ上の脆弱性把握、③マルウェアの製作、マルウェアを混入したWebページ製作、④C&Cサーバ群の準備、攻撃関連のツール準備等

（2）初期潜入：①公開メールアドレス向け標的型メールの送信、②リンクしたWebページ閲覧によるマルウェア感染後、C&Cサーバとバックドア通信によりメール取得ツールをダウンロードし、電子メール情報窃取、③個人メールアドレス向け標的型メールの作成と送信

（3）攻撃基盤構築:①マルウェア感染後C&Cサーバとバックドア通信により攻撃ツールのダウンロードと動作指示、マルウェアの更新による機能追加、②マルウェアの拡散と目標とするファイルサーバ探索

（4）攻撃目的遂行:①機密情報の窃取(ファイルサーバから窃取したデータを情報送信用端末に移動)、②機密情報の外部送信(圧縮・分割など)

2．日本年金機構への情報漏洩事件について

昨年６月に公表された日本年金機構への標的型攻撃は、社会に大きな衝撃を与えました。この事件は実際どのように攻撃されたのか、標的型攻撃メールとマルウェア（Emvidi亜種）の特徴、について確認をしました。

先ず、公開メールアドレスへのリンク(マルウェア混入した商用オンラインストレージ)によりマルウェアを感染させた後に電子メール情報を窃取。その電子メールアドレス宛に、マルウェア付きの標的型攻撃メールを送信した。このマルウェアは、従来から存在が確認されていた「Emvidi」を標的の組織向けに改良した亜種であり、検出し難く、また、lzh圧縮(脆弱性が発見されている圧縮ソフトウェア)のため、更に検出

が難しくなっています。

次に、政府のサイバーセキュリティ戦略本部より公表されている「日本年金機構における個人情報流出事案に関する原因究明調査結果」の組織のネットワーク構成から、脆弱性が何処にあるかについて、参加の皆様と確認しました。

インターネットや電子メールを接続しない、業務系パソコンで個人情報を取り扱う業務を行うことになっているが、インターネットや電子メールを接続する情報系でエクセルなどを活用し個人情報を取り扱っていたという業務運営上の脆弱性により、情報が窃取されたと考えられます。ただし、ファイアウォール（FW）やプロキシサーバが正常に機能していたという疑問がありますが、この点について、マルウェア（Emvidi亜種）のRAT（Remote Administration Tool)通信がCONNECT接続によりトンネリングし、FWやプロキシサーバを通過したと推測しました。

3．ユーザの対策について

標的型攻撃メールについては、見分けが困難なメールや添付ファイルも存在するため、マルウェア感染が避けられないことを前提に、内部・出口対策により情報漏洩を防止することが肝要と考えます。

日本年金機構の場合は、NISC(内閣官房情報セキュリティセンター)の指導がなければ更に被害が拡大していたと考えます。また、標的型攻撃実施者は、国家関与も疑われるため、十分な予算・要員・設備により、標的型メール、マルウェア、ツール、C&Cサーバ群とRAT通信など、充実が図られていると考えます。一方、組織・企業では、限られた予算・要員・設備で運営を行う必要があり、「多層防御(組織体制、情報収集、抑止機構、防御・検知機能、事故対応、復旧対応、評価予算、社員教員) [出典:「標的型攻撃 対策指南書」（株）ラック]」を基本に、被害を可能な限り小さく止めることが重要と考えます。

【参考文献】

- 「日本年金機構における個人情報流出事案に関する原因究明調査結果」
  平成27年8月20日　サイバーセキュリティ戦略本部
  http://www.nisc.go.jp/active/kihon/pdf/incident_report.pdf
- 「標的型攻撃 対策指南書」第1版　2015年7月28日　株式会社ラック
  http://www.lac.co.jp/anti-apt/

以上

☞ 関連記事： 投稿 P.5

<目次>

2016.4

注目情報（2016.3～2016.4）

■「情報セキュリティ管理基準（平成28年改正版）」策定【経済産業省】

3月1日、情報セキュリティマネジメントに関わる国際規格（ISO27001、27002）が改正されたことに基づき、経済産業省は、「情報セキュリティ管理基準（平成28年改正版）」を策定しました。

http://www.meti.go.jp/press/2015/03/20160301001/20160301001.html

■ 国内初　安全・安心なIoT製品の実現に向けた17の開発指針を公開【ＩＰＡ】

3月24日、ＩＰＡ（独立行政法人情報処理推進機構、理事長：富田達夫）技術本部ソフトウェア高信頼化センターは、今後ますます拡大が予想されるIoT製品の安全性やセキュリティの確保を目的に、IoT製品の開発者が開発時に考慮すべきリスクと対策を「つながる世界の開発指針」として策定し、ＩＰＡのウェブサイト上（https://www.ipa.go.jp/about/press/20160324.html）に公開しました。

IoT製品を開発する企業全体の「方針」の策定、つながる場合のリスクの「分析」、リスクへの対策を行うための「設計」、製品導入後の「保守」や「運用」といった製品の開発ライフサイクル全体において考慮すべきポイントを全17の指針として明示しています。（下表）

大項目		指針
方針	つながる世界の安全安心に企業として取り組む	指針１　安全安心の基本方針を策定する
		指針２　安全安心のための体制・人材を見直す
		指針３　内部不正やミスに備える
分析	つながる世界のリスクを認識する	指針４　守るべきものを特定する
		指針５　つながることによるリスクを想定する
		指針６　つながりで波及するリスクを想定する
		指針７　物理的なリスクを認識する
設計	守るべきものを守る設計を考える	指針８　個々でも全体でも守れる設計をする
		指針９　つながる相手に迷惑をかけない設計をする
		指針 10 安全安心を実現する設計の整合性をとる
		指針 11 不特定の相手とつなげられても安全安心を確保できる設計をする
		指針 12 安全安心を実現する設計の検証・評価を行う
保守	市場に出た後も守る設計を考える	指針 13 自身がどのような状態かを把握し、記録する機能を設ける
		指針 14 時間が経っても安全安心を維持する機能を設ける
運用	関係者と一緒に守る	指針 15 出荷後も IoT リスクを把握し、情報発信する
		指針 16 出荷後の関係事業者に守ってもらいたいことを伝える
		指針 17 つながることによるリスクを一般利用者に知ってもらう

表　開発指針一覧

☞ 関連記事：投稿 P.5

<目次>

2016.4

【協会主催イベント・セミナーのご案内】

■SAAJ 月例研究会（東京）

第213回	日時：2016年 5月 26日（木曜日）18:30～20:30 場所：機械振興会館 地下2階ホール	
	テーマ	「IoTって何？～IoTによるイノベーションとその課題～」（仮題）
	講師	独立行政法人情報処理推進機構(IPA) 調査役　田丸 喜一郎　氏
	講演骨子	詳細確定次第、ＨＰでご案内いたします。

■ＳＡＡＪシステム監査実践セミナー（東京）

第28回	日時：2016年 5月 26日（木曜日）～5月27日（金曜日）日帰り 9:30～17:00（進行状況により若干の変更が生じる場合があります。） 場所：晴海グランドホテル（申込み状況により変更する場合があります）	
	概要	当協会のシステム監査事例研究会「システム監査普及サービス」で実施したシステム監査事例を教材として、ロールプレイングを中心とした演習によりシステム監査を修得することを狙いとしたきわめて実践的なコースです。
	お申込み	ＨＰでご案内中です。 http://www.saaj.or.jp/kenkyu/jissenseminar/jissenseminar28.html

■ＳＡＡＪシステム監査事例セミナー（大阪）

半日コース	日時：2016年 6月 18日（土曜日）13:00～17:00 場所：大阪大学　中之島センター	
	概要	システム監査のポイントや具体的な取組方法、監査の品質・効率向上への課題などについて、内部監査事例、外部監査事例、個人情報保護、ISO 審査事例の多様な事例を、実務に携わった講師陣がご説明します。
	お申込み	ＨＰでご案内中です。 http://www.saaj.or.jp/shibu/kinki/jirei20160618.html

【外部主催イベント・セミナーのご案内】

■システム監査学会　研究大会（東京）

第30回	日時：2016年 6月 3日（金曜日）10:00～17:00 場所：機械振興会館 ホール他	
	統一論題	サイバー社会とシステム監査
	基調講演	「サイバー社会とフォレンジックについて」 講師：株式会社ＫＰＭＧ　ＦＡＳ　パートナー　伊藤益光氏
	お申込み	ＨＰでご案内中です。 http://www.sysaudit.gr.jp/taikai/2016taikai.html

<目次>

2016.4

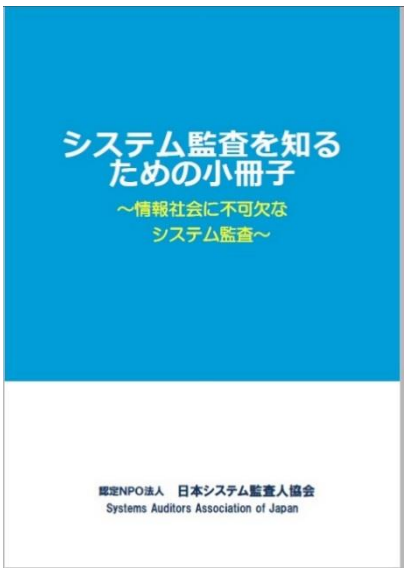
協会からのお知らせ「システム監査を知るための小冊子」（改定版）発行について

会員番号　2581 斉藤 茂雄（法人部会）

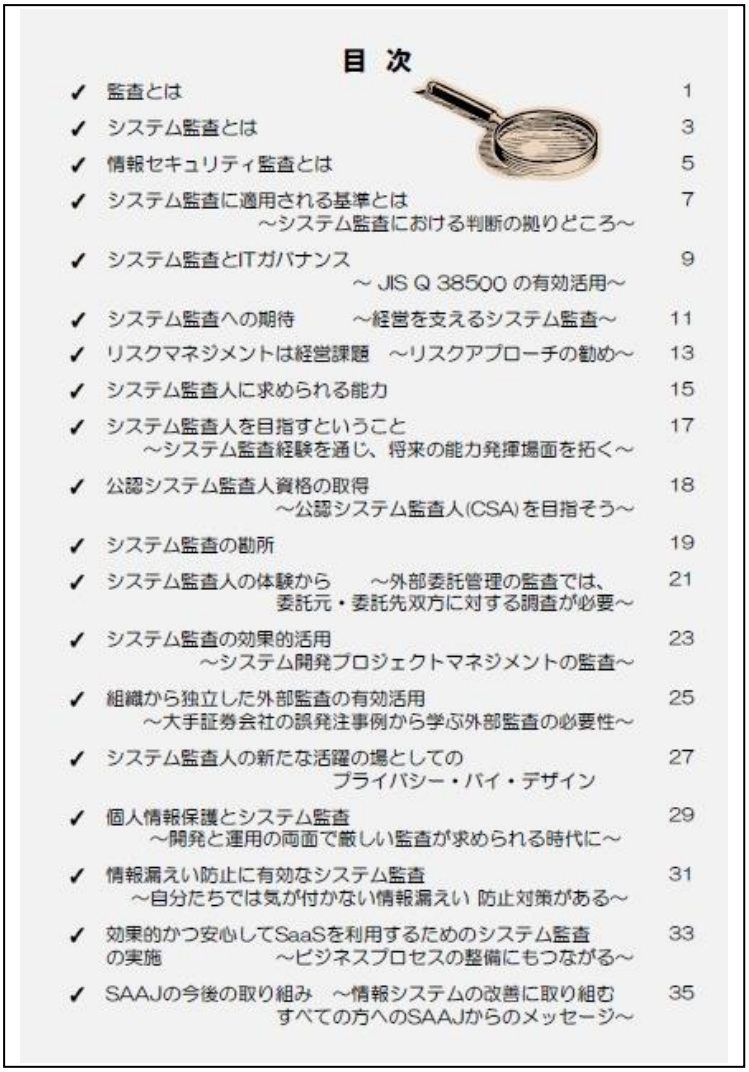
法人部会では、システム監査活性化委員会と連携して、2014 年に「システム監査を知るための小冊子～情報社会に不可欠なシステム監査～」を発行いたしましたが、この度小冊子の改訂版を発行いたしました。

小冊子の初版は、システム監査とあまり縁の無い方も対象に、全体を「入門編」と「応用編」に分けて構成しましたが、今回はより詳しくシステム監査を知っていただくことを狙いに、特に内容のレベルを意識せずまとめました。文字数も初版の２~3 割増にし、ページ数も４ページ増量しました。

本書の狙いは、「システム監査についての疑問、意義、効果、事例などを分かり易く紹介した小冊子を発行することで、システム監査の理解を助け、活性化に繋げる。併せて協会の知名度を向上させる。」ことにあります。



小冊子は A5 版表紙込み 40 ページ、中綴じカラー印刷のコンパクトなものですので、セミナー会場や企業内など、様々な場面で広くお配りいただくと、システム監査の普及、協会の知名度向上に役立つものと考えます。


目 次

最後に、発行にご協力いただいた主な方のお名前を記させていただいて、感謝申し上げます。

【執筆者（五十音順、敬称略）】梅津尚夫、小野修一、勝田敦彦、木村裕一、斉藤茂雄、斎藤由紀子、仲厚吉、中山孝明、沼野伸生、濱崎元伸、原田憲幸、藤野明夫、矢野一男

【改訂版の主な編集ご協力者（五十音順、敬称略）】安部晃生、大石正人、大西智、加佐見明夫、苅田朝子、舘岡均、力利則、樋口勝彦、藤澤博、柳田正

※小冊子は協会 HP からもご覧いただけます。
URL　http://www.saaj.or.jp/csa/system_audit_booklet2016.pdf

<目次>

2016.4

【 新たに会員になられた方々へ 】

新しく会員になられたみなさま、当協会はみなさまを熱烈歓迎しております。
協会の活用方法や各種活動に参加される方法などの一端をご案内します。

・ホームページでは協会活動全般をご案内　http://www.saaj.or.jp/index.html
・会員規程　http://www.saaj.or.jp/gaiyo/kaiin_kitei.pdf
・会員情報の変更方法　http://www.saaj.or.jp/members/henkou.html

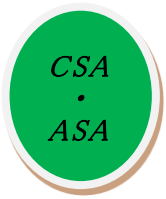
・セミナーやイベント等の会員割引や優遇　http://www.saaj.or.jp/nyukai/index.html
公認システム監査人制度における、会員割引制度など。

・各支部・各部会・各研究会等の活動。　http://www.saaj.or.jp/shibu/index.html
皆様の積極的なご参加をお待ちしております。門戸は広く、見学も大歓迎です。

・皆様からのご意見などの投稿を募集。
ペンネームによる「めだか」や実名投稿には多くの方から投稿いただいております。
この会報の「会報編集部からのお知らせ」をご覧ください。

・「情報システム監査実践マニュアル」「６か月で構築する個人情報保護マネジメントシステム」などの協会出版物が会員割引価格で購入できます。
http://www.saaj.or.jp/shuppan/index.html

・月例研究会など、セミナー等のお知らせ　http://www.saaj.or.jp/kenkyu/index.html
月例研究会は毎月100名以上参加の活況です。過去履歴もご覧になれます。



・公認システム監査人へのSTEP-UPを支援します。
「公認システム監査人」　と「システム監査人補」で構成されています。
監査実務の習得支援や継続教育メニューも豊富です。
CSAサイトで詳細確認ができます。　http://www.saaj.or.jp/csa/index.html

・会報のバックナンバー公開　http://www.saaj.or.jp/members/kaihou_dl.html）
電子版では記事への意見、感想、コメントを投稿できます。
会報利用方法もご案内しています。http://www.saaj.or.jp/members/kaihouinfo.pdf

・お問い合わせページをご利用ください。　http://www.saaj.or.jp/toiawase/index.html
各サイトに連絡先がある場合はそちらでも問い合わせができます。

<目次>

【　ＳＡＡＪ協会行事一覧　】　赤字：前回から変更された予定　　2016.4

2016	理事会・事務局・会計	認定委員会・部会・研究会	支部・特別催事
4 月	14：理事会 30：法人住民税減免申請	初旬：新規 CSA・ASA 書類審査 中旬：新規ＡＳＡ認定証発行 25：第 212 回月例研究会	17：春期情報技術者試験
5 月	12：理事会 26：年会費未納者宛督促メール発信	中旬：新規 CSA 面接 26：第 213 回月例研究会 26～27：第 28 回システム監査 実務セミナー（2 日間コース）	
6 月	2：会費未納者督促状発送 9：理事会 10～：会費督促電話作業（役員） 30：支部会計報告依頼（〆切 7/14） 30：助成金配賦額決定（支部別会員数）	10：　CSA 面接結果通知	2015/6/3：認定 NPO 法人 東京都認定日
7 月	5：支部助成金支給 14：理事会	1：秋期 CSA・ASA 募集案内 〔申請期間 8/1～9/30〕 20：認定委員会：CSA 認定証発送	14：支部会計報告〆切
8 月	（理事会休会） 27：中間期会計監査	1：秋期 CSA・ASA 募集開始～9/30	
9 月	14：　理事会		
2015	**過去に実施した行事一覧**		
10 月	8：　理事会	23：　第 207 回月例研究会	18：　秋期情報処理技術者試験
11 月	12：　理事会 13：　予算申請提出依頼（11/30〆切） 支部会計報告依頼（1/8〆切） 18：　2016 年度年会費請求書発送準備 25：　会費未納者除名予告通知発送 30：　本部・支部予算提出期限	中旬：秋期 CSA 面接 19：　第 208 回月例研究会 20：　CSA・ASA 更新手続案内 〔申請期間 1/1～1/31〕 27：　CSA 面接結果通知	2016 年 5-6：西日本支部合同研究会 （開催場所：松江）
12 月	1：　2016 年度年会費請求書発送 2016 年度予算案策定 10：　理事会：2016 年度予算案 会費未納者除名承認 第 15 期総会審議事項確認 11：　総会資料提出依頼（1/8〆切） 15：　総会開催予告掲示 18：　2015 年度経費提出期限	10：　CSA/ASA 更新手続案内メール 14：　第 209 回月例研究会 18：　秋期 CSA 認定証発送	
1 月	8：　総会資料（〆）16：00 13：　総会・役員改選の公示 14：　理事会：通常総会資料原案審議 20：　2015 年度決算案 23：　2015 年度会計監査 28：　総会申込受付開始（資料公表） 31：　償却資産税・消費税	1-31：CSA・ASA 更新申請受付 20：　春期 CSA・ASA 募集案内 〔申請期間 2/1～3/31〕 21：　第 210 回月例研究会	8：　会計：支部会計報告期限 25：　SAAJ 創立記念日
2 月	4：理事会：通常総会議案承認 25：法務局：資産登記、活動報告提出 理事変更登記 29：年会費納入期限	1～3/31：CSA・ASA 春期募集	22：第 15 期通常総会 特別講演 個人情報保護委員会 委員長　堀部　政男　氏
3 月	1：NPO 事業報告書、役員変更届東京都へ 提出 7：年会費未納者宛督促メール発信 10：理事会	2：第 211 回月例研究会 5-6：第 27 回システム監査 実務セミナー(前半) 上旬：CSA・ASA 更新認定書発送 19-20：第 27 回システム監査 実務セミナー(後半)	

<目次>

2016.4

【 会報編集部からのお知らせ 】

1．会報テーマについて
2．会報記事への直接投稿（コメント）の方法
3．投稿記事募集

□■ 1． 会報テーマについて

2016 年度の年間テーマは「システム監査の活性化」です。システム監査の活性化について、皆様といっしょに考えてみたいと思います。今月号から 7 月号までの四半期テーマを「システム監査の多様性」としました。情報システムが高度化し適用範囲が広がるに従って、情報システム関連の評価に対する要求も高度化・多様化し、システム監査においても従来と違う視点が求められています。システム監査が多様化してきている現状に対し、会員各位の意見を募るべく、四半期テーマとしました。

システム監査人にとって、報告や発表の機会は多く、より多くの機会を通じて表現力を磨くことは大切なスキルアップのひとつです。良識ある意見をより自由に投稿できるペンネームの「めだか」として始めたコラムも、投稿者が限定されているようです。また記名投稿のなかには、個人としての投稿と専門部会の報告と区別のつきにくい投稿もあります。会員相互のコミュニケーション手段として始まった会報誌は、情報発信メディアとしても成長しています。

会報テーマは、皆様のご投稿記事づくりの一助に、また、ご意見やコメントを活発にするねらいです。会報テーマ以外の皆様任意のテーマももちろん大歓迎です。皆様のご意見を是非お寄せ下さい。

□■ 2． 会報の記事に直接コメントを投稿できます。

会報の記事は、
1．PDF ファイルを、URL（ http://www.skansanin.com/saaj/ ）へアクセスして、画面で見る
2．PDF ファイルを印刷して、職場の会議室で、また、かばんにいれて電車のなかで見る
3．会報 URL（ http://www.skansanin.com/saaj/ ）の個別記事を、画面で見る

など、環境により、様々な利用方法をされていらっしゃるようです。

もっと突っ込んだ、便利な利用法はご存知でしょうか。気にいった記事があったら、直接、その場所にコメントを記入できます。著者、投稿者と意見交換できます。コメント記入、投稿は、気になった記事の下部コメント欄に直接入力し、投稿ボランをクリックするだけです。動画でも紹介しますので、参考にしてください。

（ http://www.skansanin.com/saaj/ の記事、「コメントを投稿される方へ」 ）

□■ 3．会員の皆様からの投稿を募集しております。

分類は次の通りです。
1．めだか　　：Word の投稿用テンプレート（毎月メール配信）を利用してください。
2．会員投稿　　：Word の投稿用テンプレート（毎月メール配信）を利用してください。
3．会報投稿論文：「会報掲載論文募集要項」及び「会報掲載論文審査要綱」をご確認ください。

□■ **会報投稿要項　（2015.3.12 理事会承認）**

・投稿に際しては、Word の投稿用フォーム（毎月メール配信）を利用し、
　　会報部会（saajeditor@saaj.jp）宛に送付して下さい。
・原稿の主題は、定款に記載された協会活動の目的に沿った内容にして下さい。
・特定非営利活動促進法第２条第２項の規定に反する内容(宗教の教義を広める、政治上の主義を推進・支持、又は反対する、公職にある者又は政党を推薦・支持、又は反対するなど)は、ご遠慮下さい。
・原稿の掲載、不掲載については会報部会が総合的に判断します。
・なお会報部会より、表現の訂正を求め、見直しを依頼することがあります。また内容の趣旨を変えずに、字体やレイアウトなどの変更をさせていただくことがあります。

会報記事への投稿の締切日は、毎月 15 日です。

バックナンバーは、会報サイトからダウンロードできます（電子版ではカテゴリー別にも検索できますので、ご投稿記事づくりのご参考にしてください）。

会報編集部では、電子書籍、電子出版、ネット集客、ネット販売など、電子化を背景にしたビジネス形態とシステム監査手法について研修会、ワークショップを計画しています。研修の詳細は後日案内します。

会員限定記事

【本部・理事会議事録】（会員サイトから閲覧ください。会員パスワードが必要です）

https://www.saaj.or.jp/members_site/KaiinStart

＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝＝

■発行：認定 NPO 法人　日本システム監査人協会　会報編集部
〒103-0025　東京都中央区日本橋茅場町２－８－８共同ビル６F
■ご質問は、下記のお問い合わせフォームよりお願いします。
【お問い合わせ】　http://www.saaj.or.jp/toiawase/
■会報は、会員宛の連絡事項を記載し登録メールアドレス宛に配信します。登録メールアドレス等を変更された場合は、会員サイトより訂正してください。
■会員以外の方は、購読申請・解除フォームに申請することで送付停止できます。
【会員以外の方の送付停止】　http://www.skansanin.com/saaj/register/

■□■ＳＡＡＪ会報担当
編集委員：　藤澤博、安部晃生、久保木孝明、越野雅晴、桜井由美子、高橋典子
編集支援：　仲厚吉　（会長）、各支部長
投稿用アドレス：　saajeditor ☆ saaj.jp　（☆は投稿時には@に変換してください）

<目次>